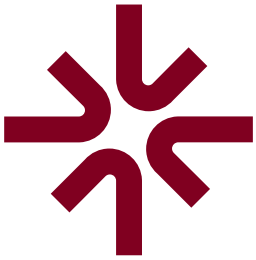


PIFAGORUS

# Technical integration with **Google Pay™**

# Table of contents

# 1. General information

Google Pay™ is an easy, fast, and, that most important, secure way to pay for your purchases in online-stores and apps. When paying through the Google Pay™ service, the card number (PAN) is not transmitted; instead, the generated virtual account number (DPAN) is used in encrypyed manner.

Before starting the integration, you need to familiarize yourself with two general documents provided by Google itself for customers who want to use their services:

**Terms of Service**
**Acceptable Use Policy**

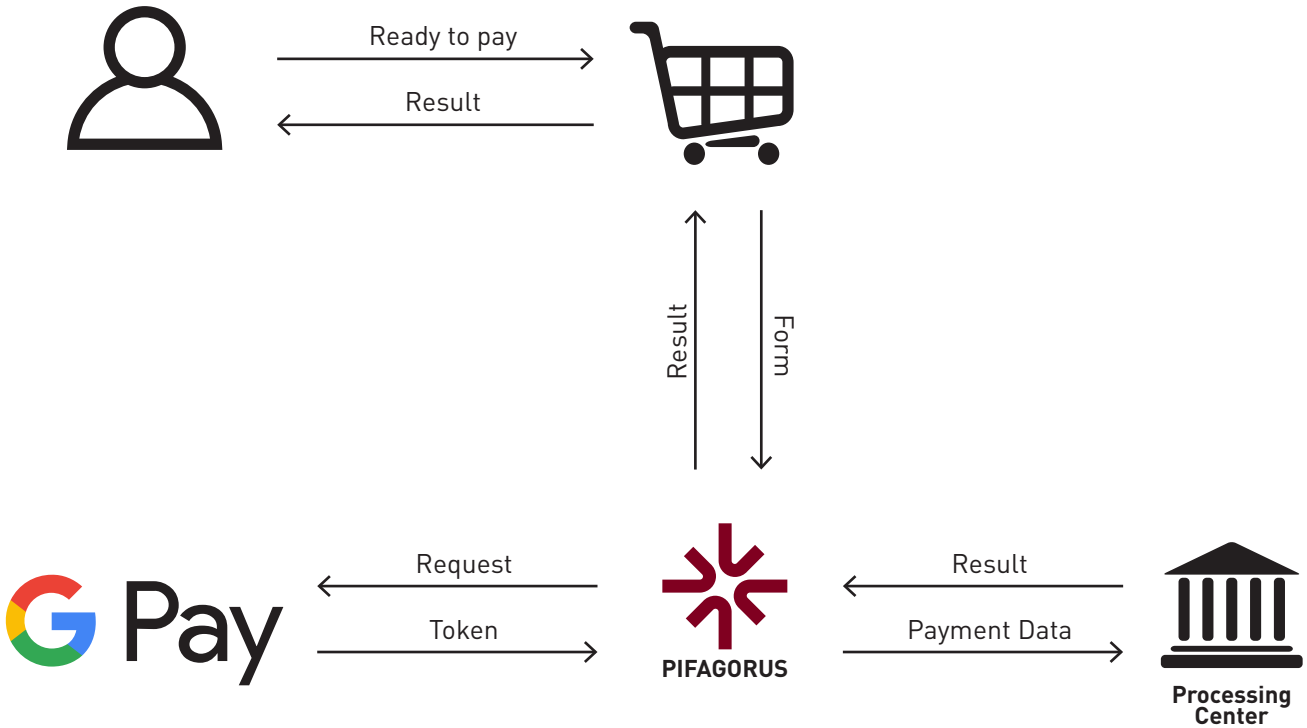
Pifagorus is working with Visa© and Mastercard© payments card networks only at the moment, with cards issued form all banks over the World except **restricted and sanctioned countries**, list of such is monitored daily and changed time to time in accordance with Pifagorus AML rules.

Pifagorus accepts every type of authorisation supported by card networks, but reserves rights to limit authorisation to more strict levels such Force 3D based on AML rules.

# 2. Integration with Google Pay™ through Pifagorus payment page

If you use the Pifagorus payment page, then additional registration in Google services is not required, just **leave a request** to connect Google Pay™ on our website.

When you use the Pifagorus payment page, the device will be automatically checked the possibility of paying through the Google Pay™ service. The button “Pay with Google Pay™” will be displayed, if the client’s device or browser supports this feature.

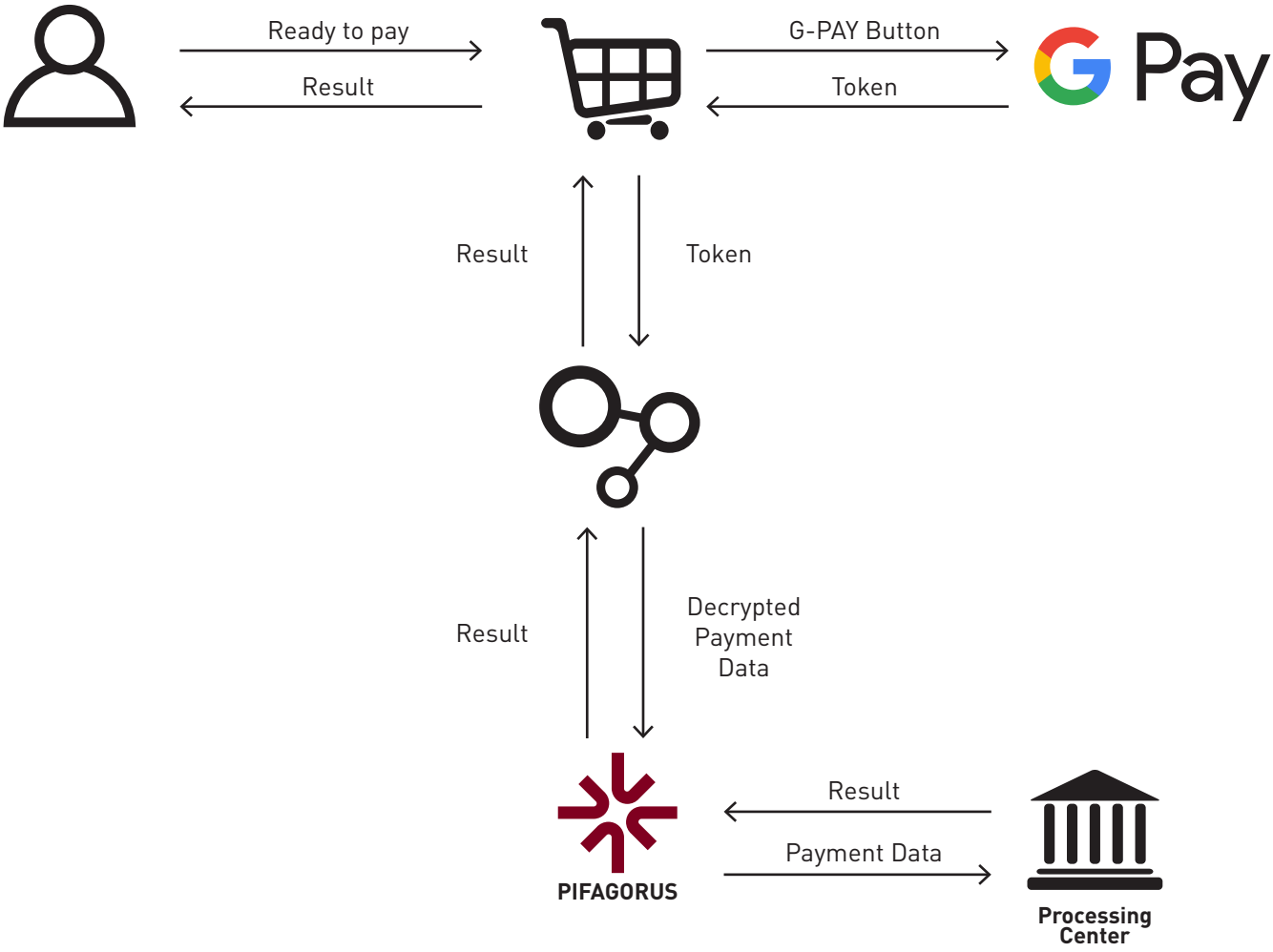


# 3. Server-to-server integration (for TPP)

With such an integration, you will need to register with the Google Pay™ service.

If you are considering not transferring the token, and decrypting it yourself using the tools of your services, then you will need to transfer the decrypted data in the API request in the secure3d parameter.

| Name | Description |
|---|---|
| secure3d | Authentification data for 3-D Secure (*) |
| *.dsrp | DSRP payment attribute |
| *.xis | PaRes Transaction ID (XID) |
| *.cavv | CAVV from PaRes |
| *.eci | ECI attribute |
| dsrp_type | Type of the DSRP payment system. Available types: masterpass, apple_pay, android_pay, samsung_pay |

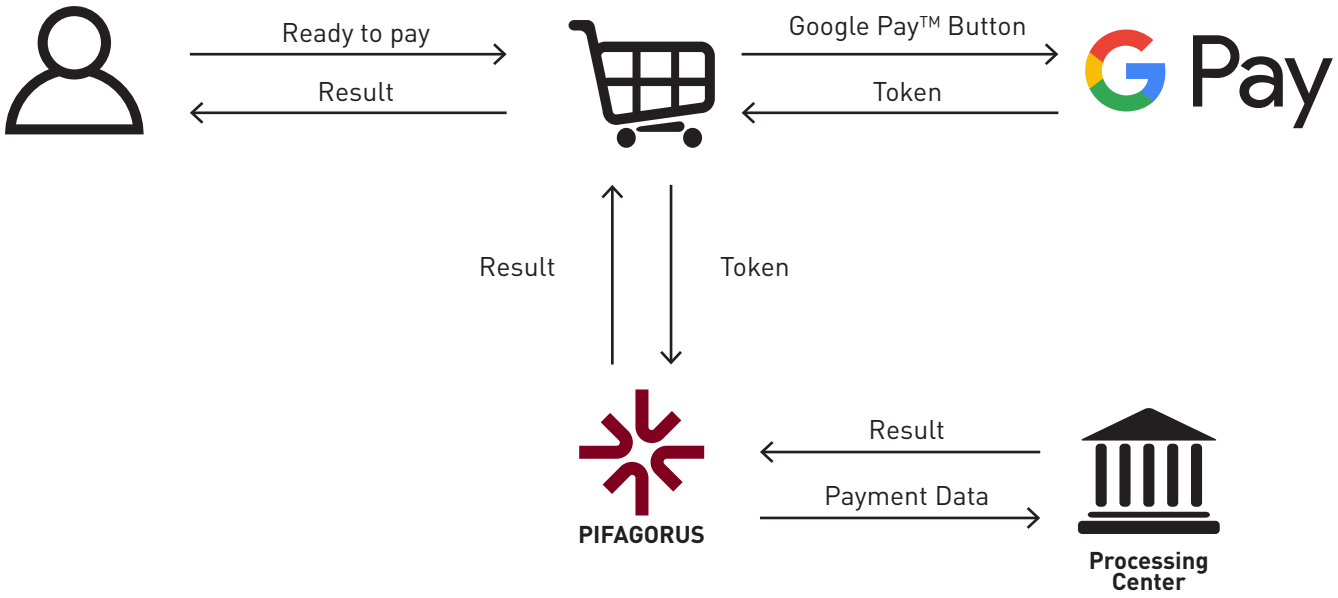


# 4. Integration with the seller's website (Tokenpay)

For working with this type of integration, you also need full integration in the Google Pay™ service. After going through full integration cycle, the seller needs to transfer only the received token from his website.

**Integration process:**

1. Get from Pifagorus Support team GatewayMerchantID;
2. Register as a **Developer** on the Google Pay™ portal;
3. Carry out a full cycle of integration with Google Pay™ on your website;
4. Pass testing and get commercial access to Google Pay™;
5. Submit the necessary information for integration to Pifagorus for setup.




After receiving the token from Google Pay™ on their website, the merchant passes it to the Pifagorus payment gateway via an API request. Then the token is decrypted and the result will sent back.

The operation of this method is described in the API documentation **(Integration_Reference)** in the section "Authorization with the transfer of an encrypted token (POST /orders/token_pay)"

# 5. Recurring payments

The method is described in the main API documentation **(Integration_ Reference)** in article: Actions -> Working with orders -> Repeating payment (POST orders /: id / rebill)

# 6. Payments with 3-D Secure for Google Pay™

Google Pay™ uses 2 types of cards:
- CRYPTOGRAM_3DS - cards that are stored as tokens on a specific user's device. The token stores the virtual card number and expiration date, so such cards do not participate in 3-D Secure verification.
- PAN_ONLY - cards available on any user's devices. The token stores the data of the physical card: number and expiration date, so 3-D Secure authentication is required for this type of cards.

The procedure for 3-D Secure authentication does not differ from the standard and described in API documentation **(Integration_Reference)** in the Actions -> Working with orders -> Authorize (Publish / Orders / Authorize) section.

## Google Pay™ API configuration code snippet sample (JSON)

```
{
  "type": "CARD",
  "parameters": {
    "allowedAuthMethods": ["PAN_ONLY", "CRYPTOGRAM_3DS"],
    "allowedCardNetworks": ["VISA", "MASTERCARD"]
  },
  "tokenizationSpecification": {
    "type": "PAYMENT_GATEWAY",
    "parameters": {
      "gateway": "<your Google-registered gateway name>",
      "gatewayMerchantId": "<GatewayMerchantID provided by PSP>"
    }
  }
}
```

Supported authentication methods:
- PAN_ONLY
- CRYPTOGRAM_3DS

Supported card networks:
- VISA
- MASTERCARD

Where:
- gateway is the Google Pay™ gateway identifier registered for the PSP;
- gatewayMerchantId is the merchant identifier issued by the PSP for Google Pay™ integration.

# 7. Additional

Billing address is always required by Pifagorus AML rules and need to be set in every request for payment initialisation **(Integration_Reference)**.

### Google Pay™ Web developer documentation
https://developers.google.com/pay/api/web/

### Google Pay™ Web integration checklist
https://developers.google.com/pay/api/web/guides/test-and-deploy/integration-checklist

### Google Pay™ Web Brand Guidelines
https://developers.google.com/pay/api/web/guides/brand-guidelines

Terms of Service:
**https://payments.developers.google.com/terms/sellertos**

Acceptable Use Policy:
**https://payments.developers.google.com/terms/aup**